UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JOHN MCLAUGHLIN, individually and on behalf of all others similarly situated, Plaintiff, v. GREYLOCK MCKINNON ASSOCIATES, INC., Defendant.	Case No. CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff John McLaughlin ("Plaintiff") brings this class action against Defendant Greylock McKinnon Associates, Inc. ("Greylock McKinnon" "Defendant") for its failure to properly secure and safeguard Plaintiff's and Class Members' protected health information ("PHI") and personally identifiable information ("PII") stored within Defendant's information network.

INTRODUCTION

1. Defendant is a consulting firm based in Boston Massachusetts, that provides expert economic analysis and litigation support to a diverse group of domestic and international clients in the legal profession, the business community, and government agencies.[1]

2. Defendant acquired, collected, and stored Plaintiff's and Class Members' PHI/PII.

[1] *See* https://www.gma-us.com/ (last accessed on April 17, 2024).

3. At all relevant times, Defendant knew or should have known, that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII.

4. On April 5, 2024, Greylock McKinnon, filed a notice of data breach with the Attorney General of Maine after discovering that the company was the recent target of a cyberattack.[2]

5. On no later than May 30, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII as hosted with Defendant, with the intent of engaging in the misuse of the PHI/PII, including marketing and selling Plaintiff's and Class Members' PHI/PII.

6. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is approximately 341,650[3] individuals.

7. Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"), which may include test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

8. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security

[2] *See* https://www.jdsupra.com/legalnews/greylock-mckinnon-notifies-341-650-of-6232827/ (last accessed on April 17, 2024).
[3] *Id.*

numbers, passport numbers, driver's license numbers, financial account numbers).

9. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendant's information network, includes, without limitation: personal and Medicare information, including names, Social Security numbers or Individual Taxpayer Identification numbers, dates of birth, mailing addresses, telephone numbers, Medicare Beneficiary Identifiers (MBI) or Health Insurance Claim Numbers (HICN), driver's license numbers and state identification numbers, healthcare providers and prescription information, health insurance claims and policy/subscriber information.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

11. As a result, the PHI/PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

12. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity

jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

14. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

15. Defendant is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant does business in this Judicial District.

THE PARTIES

Plaintiff John McLaughlin

17. Plaintiff John McLaughlin is an adult individual and, at all relevant times herein, a resident and citizen of New Jersey, residing in Woolwich Township, New Jersey. Plaintiff is a victim of the Data Breach.

18. Plaintiff's information was stored with Defendant as a result of their dealings with Defendant.

19. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive health and personal information, who then possessed and

controlled it.

20. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

21. At all times herein relevant, Plaintiff is and was a member of the Class.

22. Plaintiff received a letter from Defendant, dated April 5, 2024, stating that their PHI/PII was involved in the Data Breach (the "Notice").

23. Plaintiff was unaware of the Data Breach until receiving that letter.

24. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

25. Plaintiff was also injured by the material risk to future harm they suffer based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers and healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

26. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

27. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of

privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PHI/PII.

28. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

29. Plaintiff has a continuing interest in ensuring that their PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant Greylock McKinnon Associates, Inc.

30. Defendant Greylock McKinnon Associates, Inc., is a Massachusetts corporation with its principal place of business at 75 Park Plaza, 4th Floor, Boston, MA 02116.

CLASS ACTION ALLEGATIONS

31. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themself and the following Class:

> All individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant on May 30, 2023.

32. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and

all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

33. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

34. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

35. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible.

36. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PHI/PII;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security

measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

37. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

38. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

39. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

40. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

41. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

42. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

43. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

44. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

45. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Defendant's Failed Response to the Breach

46. Not until after months it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was potentially compromised as a result of the Data Breach.

47. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the Data Breach on May 30, 2023, and completed a review thereafter.

48. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII with the intent of engaging in the misuse of the PHI/PII, including marketing and selling Plaintiff's and Class Members'

PHI/PII.

49. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

50. Plaintiff and Class Members were required to provide their PHI/PII to Defendant as a result of their dealings, and in furtherance of this relationship, Defendant created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

51. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PHI/PII going forward.

52. Plaintiff and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

53. Unauthorized individuals can now easily access the PHI/PII and/or financial information of Plaintiff and Class Members.

Defendant Collected/Stored Class Members' PHI/PII

54. Defendant acquired, collected, and stored and assured reasonable security over Plaintiff's and Class Members' PHI/PII.

55. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PHI/PII.

56. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

57. By obtaining, collecting, and storing Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PHI/PII from unauthorized disclosure.

58. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII.

59. Plaintiff and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

60. Defendant could have prevented the Data Breach, which began no later than May 30, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PHI/PII.

61. Defendant's negligence in safeguarding Plaintiff's and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

62. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PHI/PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

63. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties it owes Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Members' data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

64. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

65. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

66. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

67. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

68. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

69. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

70. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

71. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of the breach."

72. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or

affecting commerce."[4]

73. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

74. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII of Plaintiff and Class Members.

75. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PHI/PII was adequately secured and protected.

76. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

77. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

78. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

79. Defendant owed a duty to Plaintiff and Class Members to disclose if its

[4] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

computer systems and data security practices were inadequate to safeguard individuals' PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendant.

80. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

81. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

82. PHI/PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

83. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[5]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[6]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[7]

84. Identity thieves can use PHI/PII, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed April 16, 2024).
[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed April 16, 2024).
[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed April 16, 2024).

for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

85. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

86. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PHI/PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

87. As detailed above, Defendant is a sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

88. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*,

[8] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed April 16, 2024).

(i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PHI/PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

89. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

90. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PHI/PII of Plaintiff and Class Members in its computer systems and on its networks.

91. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in its possession;

b. to protect Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII.

92. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

93. Defendant knew, or should have known, of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems, and the importance of adequate security.

94. Defendant knew about numerous, well-publicized data breaches.

95. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI/PII.

96. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Plaintiff and Class Members had entrusted to it.

97. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI/PII.

98. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained therein.

99. Plaintiff's and Class Members' willingness to entrust Defendant with their PHI/PII was predicated on the understanding that Defendant would take adequate security precautions.

100. Moreover, only Defendant had the ability to protect its systems and the PHI/PII is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

101. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

102. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and

foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII of Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI/PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

103. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

104. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

105. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

106. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff

and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

107. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

108. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII.

109. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI/PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

110. Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing, and maintaining appropriate security measures.

111. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

112. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

113. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII is used; (iii) the compromise, publication, and/or theft of their PHI/PII; (iv) out-of-pocket expenses associated

with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI/PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

114. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

115. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Class)

116. Plaintiff realleges and reincorporates every allegation set forth in the preceding

paragraphs as though fully set forth herein.

117. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII.

118. Defendant required Plaintiff and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's services.

119. Defendant solicited and invited Plaintiff and Class Members to provide their PHI/PII as part of Defendant's regular business practices.

120. Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

121. As a condition of their relationship with Defendant, Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant.

122. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

123. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

124. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

125. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate

notice to them that their PHI/PII was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Class)

127. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

128. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

129. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

130. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PHI/PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

131. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

132. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

133. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

134. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PHI/PII to Defendant, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PHI/PII secure.

135. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI/PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

136. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

137. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

138. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to

make a rational and informed purchasing and servicing decision and took undue advantage of Plaintiff and Class Members.

139. Defendant was unjustly enriched at the expense of Plaintiff and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and or services that did not satisfy the purposes for which they bought/sought them.

140. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

141. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PHI/PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors

and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess

whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: April 16, 2024

Respectfully submitted,

By: */s/ James J. Reardon*

James J. Reardon (BBO# 566161)
REARDON SCANLON LLP
45 South Main Street, 3rd Floor
West Hartford, CT 06107
T: (860) 944-9455
james.reardon@reardonscanlon.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

**Pro Hac Vice admission forthcoming*

Attorneys for Plaintiff and the Class